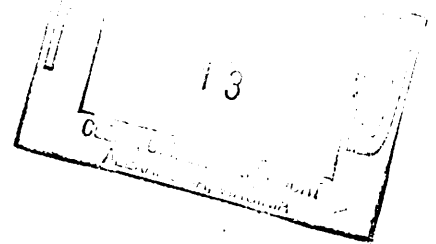


IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

CHEA S. YARL,
a/k/a "CACA S. YARL,"

CAESAR E. ADIGWE, JR,

SAMUEL B. SMITH, JR,

THOMAS GHERENSE,

Defendants.

Case No. 1:19-MJ-529

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Gregory R. Settducati, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 2012. I have experience investigating organized crime and national security matters.

2. I am currently assigned to the FBI's Washington Field Office, Northern Virginia Resident Agency, and have been so assigned since June 2012. I am currently assigned to a squad that investigates organized crime and criminal enterprises. My duties with the FBI include, but are not limited to, the investigation of alleged violations of federal criminal statutes, including bank, mail, and wire fraud, money laundering, and crimes that involve financial institutions. I have conducted physical and electronic surveillance, executed search and arrest warrants, and reviewed

and analyzed records and documents for fraudulent activity. I have interviewed suspects, defendants, witnesses, victims, and spoken to other experienced investigators concerning the methods and practices of criminal enterprises. In addition, I am a graduate of the FBI Academy, and have received training in cyber security matters.

3. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. The facts and information contained in this Affidavit are based on my training and experience, my personal knowledge, my involvement in this investigation, and information that has been provided to me by other law enforcement professionals. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by review of the records, documents, and other physical evidence obtained during the course of this investigation. In addition, where conversations or statements are related herein, they are related in substance and in part except where otherwise indicated. This Affidavit contains only the information necessary to support probable cause and is not intended to include each and every fact and matter observed by me or known to the government.

4. This Affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint and arrest warrant for CHEA S. YARL, CAESAR E. ADIGWE, JR, SAMUEL B. SMITH, JR, and THOMAS GHERENSE, and does not include all of the facts and circumstances related to this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that CHEA S. YARL, CAESAR E. ADIGWE, JR, SAMUEL B. SMITH, JR, and THOMAS GHERENSE have committed violations of Title 18, United States Code, Section 1349 (Conspiracy to Commit Bank Fraud).

OVERVIEW OF CARD CRACKING BANK FRAUD SCHEME

5. The United States Postal Inspection Service (“USPIS”), the Virginia State Police (“VSP”), and the FBI, in conjunction with other local and federal law enforcement agencies and fraud investigators at financial institutions insured by the Federal Deposit Insurance Corporation (“FDIC”) have been investigating a bank fraud scheme dubbed “card cracking.” Based on the investigation by USPIS and other law enforcement agencies, and based on my training and experience, I understand the card cracking bank fraud scheme to generally operate as follows:

6. Card cracking organizing conspirators recruit third-party bank account holders (“cardholders”) to provide their debit cards and Personal Identification Numbers (“PIN”) and account information for use in the scheme. Conspirators recruit card holders in various ways. Some conspirators recruit cardholders in person while others utilize social media platforms like Instagram or Facebook to advertise opportunities to make “quick money,” after which cardholders contact the conspirators by phone, text message, or through social media.

7. Once a cardholder has been recruited and the conspirator has secured the cardholder’s debit card and PIN, as well as one or more counterfeit checks, the conspirator deposits—or recruits someone to deposit—the counterfeit checks into the cardholder’s bank account. The conspirators typically deposit the checks through the use of an Automated Teller Machine (“ATM”).

8. The organizing conspirators manufacture, purchase, or otherwise obtain one or more counterfeit checks to deposit into the cardholder’s bank account. The counterfeit checks used in the card cracking scheme generally contain legitimate bank account and routing number information belonging to legitimate businesses who are unaware that their bank account and routing number information has been compromised.

9. Once the counterfeit checks are deposited to the cardholder’s account, the conspirator

waits for the cardholder's bank to credit the purported funds from the counterfeit check to the cardholder's account, which can happen in a matter of hours. According to information provided by bank investigators, banks typically credit the value of the check to a cardholder's account before the check actually clears, that is, before the cardholder's bank establishes the check's validity. In order to clear a check, the cardholder's bank receives an image of the check (which is sent electronically to the drawer's bank), determines whether it is valid, and requests and receives payment (or denial of payment) from the check drawer's bank. By moving forward prior to clearing the check, the cardholder's bank advances the bank's own money into the cardholder's account when a check is deposited with the risk that the check ultimately could be counterfeit or fraudulent. During the time period between the deposit of a counterfeit or fraudulent check and when the cardholder's bank learns that the check is fraudulent, the advanced money in the cardholder's bank account can be withdrawn from the account using the cardholder's debit card and PIN.

10. After one or more counterfeit checks are deposited into a third-party bank account, the card cracking conspirator often attempts a relatively small ATM withdrawal (between \$100 and \$500) a few hours later, to determine whether the bank has credited the account with the funds from the counterfeit check. If the conspirator is able to withdraw the cash at an ATM, (i.e., the bank has advanced funds to the account), the conspirator goes to a point-of-sale terminal to withdraw or spend the remaining funds that the bank advanced to the third-party account. Point-of-sale terminals are machines used to process debit and credit card payments, typically for the purchase of goods. For example, the machines at a grocery store checkout counter in which a customer swipes a debit card are point-of-sale terminals.

11. When the floated funds are withdrawn in person at a bank branch or at an ATM, and the funds are a result of a deposit of a counterfeit or fraudulent check, the FDIC-insured bank suffers

a loss when it disperses the cash to the person at a bank counter or via an ATM withdrawal.

PROBABLE CAUSE

I. CHEA S. YARL's Card Cracking Activity

12. CHEA S. YARL ("YARL"), who goes by the moniker "Los," is known to produce counterfeit checks and to use those checks to defraud financial institutions throughout Virginia, Maryland, and Washington, D.C.

13. Telephone records, bank records, surveillance footage, physical surveillance by law enforcement, and statements provided to law enforcement by cooperators, reveal that since at least 2013, YARL has participated in multiple card cracking schemes, including the production of counterfeit checks, the deposit of counterfeit checks, the withdrawal of funds associated with the deposit of counterfeit checks, and the purchase of money orders with stolen funds.

14. In February 2014, the Police Department of Edmonston, Maryland, searched YARL in connection with a traffic stop and recovered from his vehicle several counterfeit checks that appeared to belong to a public university located in Virginia. The following items were recovered from YARL's vehicle: two counterfeit checks, one made payable to A.V. in the amount of \$1,440 and one made payable to D.W. in the amount of \$2,334; a Visa debit card in the name of A.V.; a MasterCard payment card in the name of M.A.; a MasterCard payment card in the name of L.D.M.; a MasterCard payment card in the name of C.E.E.; and an iPhone belonging to YARL.

15. In March 2015, after learning about a card cracking investigation in northern Virginia, Edmonston Police Department notified the Stafford County Sheriff's Office ("SCSO") and the Virginia State Police ("VSP") about its February 2014 search of YARL and subsequently provided the items recovered from YARL's vehicle to SCSO detectives and VSP agents.

16. A forensic examination of YARL's cellular telephone, done by SCSO in June 2015

pursuant to a search warrant, revealed numerous photographs and text messages related to counterfeit checks and card cracking schemes. The review of the cellular telephone showed relevant text messages starting in September 2013 and continuing into and until February 2014, when Edmonston Police Department seized YARL's cellular telephone.

17. For example, a photograph of a Food Lion check was sent to YARL by SAMUEL B. SMITH, JR ("SMITH") via text message on September 5, 2013. Law enforcement later learned that on or about September 5, 2013, YARL presented a counterfeit Food Lion check to a financial institution located on Baltimore Avenue in Laurel, Maryland, to be deposited into an account belonging to R.P. YARL presented R.P.'s debit card and provided his own (YARL's) identification card to the employee of the financial institution. R.P.'s account had been flagged for fraud because R.P. had previously called to report his debit card lost or stolen. Upon learning that R.P.'s account had been flagged, the employee called the police at which point YARL fled without his identification card.

18. YARL's cellular telephone contained photographs of other checks as well as hundreds of text messages sent to him by co-conspirators, known and unknown, containing personal details related to many different names, including the person's street address, bank account information and the associated financial institution, and oftentimes a specified amount of money. Many of the text messages found on YARL's cellular telephone contained real time updates from co-conspirators about the deposit of counterfeit checks and subsequent withdrawal of funds related to those checks. Text messages in YARL's cellular telephone also mentioned money transfer services, such as MoneyGram and Western Union, and included reference numbers related to specific fund transfers and the purchase of money orders.

19. This investigation has revealed that since 2013, YARL has personally participated

in a conspiracy in which hundreds of counterfeit checks were deposited into accounts at financial institutions and then funds from those accounts were subsequently withdrawn.

20. For example, on or about October 1, 2015, at 4:43 p.m., YARL deposited a counterfeit check in the amount of \$3,819.46, made payable to S.A., at a financial institution located on Cherry Hill Road in Silver Spring, Maryland. On or about October 2, 2015, at 10:06 a.m., an unidentified male withdrew \$3,000 from S.A.'s account at a financial institution located on Horner Road in Woodbridge, Virginia. Surveillance footage from the financial institution located on Cherry Hill Road in Silver Spring, Maryland, captured images of YARL on October 1, 2015, depositing the check and departing the branch at approximately 4:43 p.m.

21. In 2018, a financial institution ("Company A") provided law enforcement with evidence that, from December 2017 to December 2018, at least 200 counterfeit checks had been deposited into more than 130 accounts at branches of Company A located in northern Virginia, Washington, D.C., and Maryland. Legitimate routing and account numbers belonging to cashier's accounts had been used to make the counterfeit checks. The counterfeit checks were deposited into the accounts and then funds were withdrawn from those accounts before Company A realized the checks were fraudulent. As a result of the card cracking conspiracy, Company A incurred a loss of over \$210,000 spanning the year of December 2017 to December 2018. Analysis of images of the counterfeit checks showed that the handwriting on many of the checks was similar.

22. A review of surveillance footage provided by Company A, as well as transaction records, revealed that YARL conducted the following deposits of counterfeit checks into accounts of Company A at branches located in Maryland and the Eastern District of Virginia:

23. On December 22, 2017, YARL deposited a counterfeit check in the amount of

\$1,900, made payable to D.L., into D.L.'s account at the Company A branch located on Wisconsin Avenue in Bethesda, Maryland.

24. On January 4, 2019, YARL deposited a counterfeit check in the amount of \$2,400, made payable to G.R., into G.R.'s account at the Company A branch located on Montgomery Avenue in Gaithersburg, Maryland.

25. On January 8, 2018, a counterfeit check in the amount of \$1,750, made payable to T.C., was deposited into T.C.'s account at the Company A branch located on Belcrest Center Drive in Hyattsville, Maryland. On January 9, 2018, a debit card associated with the account was used to purchase a United States Postal Service ("USPS") money order in the amount of \$750. Law enforcement subsequently obtained an image of the money order from January 9, 2018, which identifies YARL as payor.

26. On January 17, 2019, YARL deposited a counterfeit check in the amount of \$2,200, made payable to I.D., into I.D.'s account at the Company A branch located on Research Boulevard in Rockville, Maryland.

27. On January 17, 2019, YARL deposited a counterfeit check in the amount of \$2,200, made payable to D.M., into D.M.'s account at the Company A branch located on Montgomery Village Avenue in Gaithersburg, Maryland.

28. On or about January 19, 2018, YARL deposited a counterfeit check in the amount of \$3,200, made payable to J.G., into J.G.'s account at the Company A branch located on Strawberry Lane in Falls Church, Virginia, within the Eastern District of Virginia.

29. On or about January 19, 2018, YARL deposited a counterfeit check in the amount of \$2,400, made payable to H.P., into H.P.'s account at the Company A branch located on N. Glebe Road in Arlington, Virginia, within the Eastern District of Virginia.

30. On January 25, 2019, YARL deposited a counterfeit check in the amount of \$1,900, made payable to R.D., into R.D.'s account at the Company A branch located on Rockville Pike in Rockville, Maryland.

31. On or about January 26, 2018, YARL deposited a counterfeit check in the amount of \$1,900, made payable to D.M., into D.M.'s account at the Company A branch located on N. Glebe Road in Arlington, Virginia, within the Eastern District of Virginia.

32. On or about January 26, 2018, YARL deposited a counterfeit check in the amount of \$2,200, made payable to D.M., into D.M.'s account at the Company A branch located on Strawberry Lane in Falls Church, Virginia, within the Eastern District of Virginia.

33. On or about February 8, 2018, YARL deposited a counterfeit check in the amount of \$2,200, made payable to K.K., into K.K.'s account at the Company A branch located on Old Dominion Road in McLean, Virginia, within the Eastern District of Virginia.

II. SAMUEL B. SMITH, JR's Card Cracking Activity

34. Based on analysis of cellular telephone records, physical surveillance, bank records, video surveillance, and information provided to law enforcement by cooperators, SMITH recruited cardholders in furtherance of the card cracking conspiracy. SMITH repeatedly identified names and bank account information that could be used on counterfeit checks and then provided that information to his co-conspirators.

35. SMITH personally participated in the deposit of counterfeit checks and the withdrawal of funds associated with those checks in furtherance of the card cracking conspiracy. Examples of transactions in which SMITH participated are below:

36. On or about September 22, 2015, at 3:46 p.m., SMITH deposited a counterfeit check for \$3,350.86 made payable to C.W. into C.W.'s empty account at a financial institution located on

University Boulevard in Adelphi, Maryland. On or about September 23, 2015, at 9:37 a.m., SMITH withdrew \$1,600 of cash, attributable to the C.W. check deposited on September 22, 2015, from C.W.'s account at a financial institution located on Greenbelt Road in Greenbelt, Maryland. The same day, at 9:54 a.m., SMITH withdrew \$1,200 of cash from the C.W.'s account at a financial institution located on University Boulevard in Adelphi, Maryland. On or about September 23, 2015, at 3:35 p.m., a second counterfeit check for \$3,559.41, also made payable to C.W., was deposited into C.W.'s account at a financial institution located on Shady Grove Road in Gaithersburg, Maryland. Surveillance footage from the financial institution located on University Boulevard in Adelphi, Maryland, shows SMITH at the location both on September 22 and September 23, at the same times he made a deposit and subsequent withdrawal from C.W.'s account.

37. On or about October 1, 2015, at 4:10 p.m., YARL deposited a counterfeit check in the amount of \$3,795.41 made payable to M.F. into M.F.'s account at a financial institution located on Maple Lawn Boulevard in Fulton, Maryland. On or about October 2, 2015, at 10:23 a.m., SMITH withdrew \$1,800 in cash from M.F.'s account from a financial institution located on Greenbelt Road in Greenbelt, Maryland. On the same day, at 10:38 a.m., SMITH withdrew \$1,200 from the same account at a financial institution located on Greenbelt Road in College Park, Maryland. On or about October 2, 2015, at 1:32 p.m., SMITH deposited a counterfeit check in the amount of \$3,840.51, also made payable to M.F., into M.F.'s account at financial institution located on Shady Grove Road in Gaithersburg, Maryland. Surveillance footage from the financial institution located on Maple Lawn Boulevard in Fulton, Maryland, shows YARL making a deposit on October 1, 2015, at approximately 4:10 p.m. Surveillance footage from the financial institution located on Greenbelt Road in Greenbelt, Maryland, shows SMITH making a withdrawal on October 2, 2015, at approximately 10:38 a.m. Surveillance footage from the financial institution located on Shady

Grove Road in Gaithersburg, Maryland, shows SMITH making a deposit on October 2, 2015, at approximately 1:32 p.m.

III. CAESAR ADIGWE's Card Cracking Activity

38. Based on analysis of cellular telephones, physical surveillance, bank records, video footage, and information provided to law enforcement by cooperators, ADIGWE recruited cardholders in furtherance of the card cracking conspiracy. ADIGWE repeatedly identified names and bank account information that could be used for the production of counterfeit checks and then provided that information to his co-conspirators. ADIGWE also provided personal identification numbers ("PINs") from cardholders ADIGWE recruited, allowing him and his conspirators to deposit the counterfeit checks into the accounts associated with the debit cards.

39. Like YARL, ADIGWE participated in the 2018 card cracking scheme affecting Company A. Based on records provided by USPIS, from January 2018 to February 2018, ADIGWE was the payee on over \$12,000 worth of USPS money orders—all of which were purchased with debit cards for accounts with Company A that had received counterfeit checks.

40. Surveillance footage from on or about August 18, 2018, shows ADIGWE cashing a USPS money order in the amount of \$1,000 at a U.S. Post Office in Washington, D.C. The money order was purchased on December 29, 2017, with a debit card belonging to A.W. for a Company A account. A counterfeit check had previously been deposited into A.W.'s account.

IV. THOMAS GHERENSE's Card Cracking Activity

41. Based on analysis of cellular telephones, physical surveillance, bank records, and video footage, GHERENSE, together with YARL, ADIGWE, and SMITH, deposited counterfeit checks into numerous bank accounts in furtherance of the card cracking conspiracy.

42. Law enforcement reviewed an Instagram account belonging to ADIGWE, with the

username “bigcezceo,” revealing photographs of ADIGWE, YARL, and an individual identified by the Instagram username “tomgg30.”

43. A review of records obtained from Facebook concerning the Instagram account tomgg30 revealed the email address associated with the account to be thomas.gherense68@gmail.com. A search of Maryland Motor Vehicle Administration (“MVA”) records for THOMAS GHERENSE revealed a photograph of a male who law enforcement determined was the same individual identified by the username tomgg30 in Instagram photographs with ADIGWE and YARL. Law enforcement then compared the Instagram photographs and MVA photograph with video surveillance from financial institutions to determine that GHERENSE was a conspirator in the card cracking conspiracy involving YARL, ADIGWE and SMITH.

44. Like YARL and ADIGWE, GHERENSE participated in the 2018 card cracking scheme affecting Company A. A review of surveillance footage and transaction records provided by Company A revealed the following transactions conducted by GHERENSE in which he deposited counterfeit checks into multiple Company A accounts in 2018:

45. On January 26, 2018, GHERENSE deposited a \$1,900 counterfeit check made payable to T.D. into a Company A account at the branch located on Leesburg Pike in Tysons Corner, Virginia, within the Eastern District of Virginia.

46. On February 12, 2018, GHERENSE deposited a counterfeit check in the amount of \$2,412 payable D.C. into a Company A account at the branch located on Georgia Avenue in Silver Spring, Maryland.

47. On February 22, 2018, GHERENSE deposited a \$1,943 counterfeit check made payable to B.M. into a Company A account at the branch located at Spectrum Center in Reston, Virginia, within the Eastern District of Virginia.

48. On February 22, 2018, GHERENSE deposited a \$2,750 counterfeit check made payable to T.J. into a Company A account ending at the branch located on Old Dominion Drive in McLean, Virginia, within the Eastern District of Virginia.

49. On June 27, 2018, GHERENSE deposited a counterfeit check in the amount of \$1,698.11 made payable to N.V. into a Company A account at the branch located on Georgia Avenue in Silver Spring, Maryland.

50. On August 7, 2018, GHERENSE deposited a counterfeit check in the amount of \$1,983.11 made payable to J.L. into a Company A account at the branch located on Mac Arthur Boulevard NW in Washington, D.C.

51. On August 10, 2018, GHERENSE deposited a counterfeit check in the amount of \$1,943.71 made payable to S.K. into a Company A account at the branch located on Wisconsin Avenue in Bethesda, Maryland.

EXISTENCE OF A CONSPIRACY

52. Cellular telephones, physical surveillance, bank records, video footage, and statements to law enforcement by cooperators reveal that, since at least 2013, YARL, SMITH, and ADIGWE have conspired together and with other individuals, known and unknown, to deposit counterfeit checks and stolen real checks into bank accounts throughout the D.C.-metro area and to then withdraw funds from those accounts. Evidence shows that GHERENSE has participated in the card cracking conspiracy with YARL, SMITH, and ADIGWE since at least 2018.

53. As noted in paragraph 34, *supra*, SMITH recruited cardholders in furtherance of the card cracking conspiracy. SMITH repeatedly identified names and bank account information that could be used on counterfeit checks and then provided that information to YARL. Below are

examples of text messages between YARL and SMITH, at his known cellular telephone number of (XXX) XXX-1314, in which they discuss the card cracking conspiracy:

From	To	Date/Time	Text
SMITH	YARL	9/5/2013, 7:28pm	.acc# 0000XXXXXX4540 nd wat else capital one the pin: 4458
SMITH	YARL	9/5/2013, 7:28pm	Acct# XXXXXX7037 PIN# 2974 td bank
SMITH	YARL	9/6/2013, 1:03am	Aye the td she says its negative 2200
YARL	SMITH	9/6/2013, 1:03am	It should be there in the morning
SMITH	YARL	9/6/2013, 6:44pm	7107 Donnell Pl 20747 go get that pnc
YARL	SMITH	9/6/2013, 6:45pm	Dropping cap now

54. Paragraph 37, *supra*, describes how YARL and SMITH worked together on October 1, 2015, and October 2, 2015, to deposit counterfeit checks into M.F.'s account and then withdraw approximately \$3,000 from the account.

55. Paragraph 38, *supra*, describes how ADIGWE recruited cardholders in furtherance of the card cracking conspiracy. ADIGWE contacted YARL from the phone number (XXX) XXX-0847, which law enforcement confirmed belonged to ADIGWE through a booking report for ADIGWE related to a prior arrest. In one text message with YARL in 2013, ADIGWE asked YARL to make counterfeit checks for amounts below \$2,500 or \$2,600 because checks in amounts greater than that were less likely to be cleared by financial institutions. On numerous occasions, ADIGWE told YARL the amount of money ADIGWE was able to withdraw from various bank accounts. In one instance, ADIGWE notified YARL that a counterfeit check was "dead," as the financial institution told ADIGWE during his attempt to withdraw money that the "check is counterfeit."

56. Between November 2013 and February 2014, ADIGWE sent text messages to YARL containing approximately 20 names, along with the associated account information, for use in the card cracking conspiracy. In multiple texts with YARL, ADIGWE discussed obtaining and cashing a "mo," which is an abbreviation for money order. In a card cracking scheme, a compromised debit

card can be used to purchase a money order after a counterfeit check is deposited into the account associated with the debit card. The money order is then cashed. Based on my training and experience, I know that purchasing a money order can be more profitable than making a cash withdrawal from a compromised account because many financial institutions allow for only a limited amount of cash to be withdrawn from an account before the check clears. The purchase of a money order is considered to be a point-of-sale transaction and all funds deposited into the account, including from an uncleared check, are available to purchase a money order. Examples of the hundreds of text messages between ADIGWE and YARL about the card cracking scheme are below:

From	To	Date/Time	Text
ADIGWE	YARL	12/31/2013, 12:30pm	Ight bet my bad bout yesterday though crazy day. But I need to make up for it. If u have mo's for me let me know.
ADIGWE	YARL	1/1/2014, 10:26am	Text me the pins to the acs
ADIGWE	YARL	1/1/2014, 4:12pm	Ace cash checking takes \$33.33 for cashing \$1000 mo's
YARL	ADIGWE	1/1/2014, 9:09pm	Romeo:4702. Adesola:4859
ADIGWE	YARL	1/7/2014, 11:53pm	Romeo card is off and I dropped in adesola it might be there in the morning
ADIGWE	YARL	1/8/2014, 12:00am	Yeah it cleared 200 then said call institution when I tried to take it out then I went to cvs and 100 was available so I took the hundred out
ADIGWE	YARL	1/8/2014, 4:57pm	Good look I'm a just through u two ac s I'm a just pay my guy n keep the rest

57. On some occasions, three or more of the conspirators worked together to defraud the same financial institution using the same compromised accounts. A review of surveillance video and account records from a financial institution revealed that on August 27, 2015, at approximately 3:21p.m., YARL deposited a counterfeit check in the amount of \$3,883.19 into an account belonging to A.W. at the branch located on River Parkway in Columbia, Maryland. On August 28, 2015, at approximately 10:01a.m., SMITH unsuccessfully attempted to make a withdrawal from A.W.'s account at the branch located on Maple Lawn Boulevard in Fulton, Maryland. On August 28, 2015,

at approximately 5:51 p.m., ADIGWE deposited a counterfeit check in the amount of \$3,558.19 into the same account at the branch located on East West Highway in Hyattsville, Maryland. On August 28, 2015, and August 31, 2015, A.W. made cash withdrawals from his account totaling \$7,400 at the branch located on Forest Hill Avenue in Richmond, Virginia, which resulted in the financial institution sustaining a loss of \$5,000.

58. From December 2017 to December 2018, as noted throughout, YARL, ADIGWE, and GHERENSE participated in a card cracking scheme to defraud Company A, a financial institution, by depositing at least 200 counterfeit checks into, and subsequently withdrawing money from, 130 accounts.

59. In 2019, YARL, SMITH, and GHERNSE worked together to defraud Company B, a financial institution. On July 1, 2019, an employee of Company C, a home building company in Rockville, Maryland, placed 12 checks of varying amounts, in separate envelopes, into the USPS blue collection box located on New Hampshire Avenue, in Silver Spring, Maryland after the last collection time.

60. On July 12, 2019, YARL opened a business account at a Company B, under the name of Company D, a residential and commercial contractor based in Lanham, Maryland, with K.W. as the account holder. To open the account, YARL provided mobile phone number XXX-XXX-9112 and a location on Pleasant Street, Annapolis, Maryland 21401 as the address.

61. On July 15, 2019, SMITH deposited a stolen check into the Company B business account opened by YARL on July 12, 2019.¹ The stolen check was made payable to Company D

¹ A previous search warrant affidavit associated with this investigation identified the individual depositing the stolen check on July 15, 2019, as YARL. Subsequent investigation revealed the true identity of the individual to be SMITH, which was confirmed through the comparison of security camera footage with a DMV photograph.

in the amount of \$176,407.40. Subsequent investigation revealed that the stolen check belonged to Company C and was one of the checks placed in the USPS blue box by a Company C employee on July 1, 2019. Security cameras at Company B captured images of YARL opening the account and SMITH depositing the stolen check.

62. On July 17, 2019, YARL opened a business account at Company E, a financial institution, in the name of Company D with K.W. listed as the account holder. To open the account, YARL used the mobile phone number XXX-XXX-9112 and a location on Pleasant Street, Annapolis, Maryland 21401 as the address. On July 17, 2019, a starter check issued through the Company B account was used to transfer \$85,000 from the Company B account to the Company E account. An investigator for Company B flagged the Company B account due to the high value transfer of \$85,000.

63. On July 18, 2019, YARL opened a second business account at Company B. The account was opened under the name Boss Groupe LLC with K.P. listed as the account holder. To open the account, YARL used a location on Pleasant Street, Annapolis, Maryland 21401 as the address. YARL attempted to deposit a starter check in the amount of \$84,300 from the Company E account into the second Company B account. Because the first Company B account had been flagged for suspicious activity on July 17, 2019, the Company B investigator was notified of suspicious activity the next day when YARL opened the second Company B account using the same street address that he used to open the first Company B account on July 12, 2019. The investigator was able to access the live feed of Company B's security system and witnessed YARL attempt to deposit the \$84,300 starter check into the new account. The investigator directed a local branch employee to contact the Greenbelt Police Department.

64. Upon arrival, Greenbelt Police Department arrested YARL and took him into custody. During a search incident to arrest, Greenbelt Police Department seized YARL's cell phone and a fraudulent Social Security card belonging to K.W. A search of YARL's cell phone, which was done pursuant to a search warrant issued by the Eastern District of Virginia, revealed communications between YARL and the telephone number (XXX) XXX-8024. Investigators believe the phone number ending in 8024 belongs to SMITH because, on or about July 9, 2019, this number texted YARL a screenshot of a money payment app that showed the username "Samuel Smith." A query of an open source database revealed that the phone number ending in 8024 was associated with SMITH.² On or about July 15, 2019, YARL sent the following text message to (XXX) XXX-8024:

"Business name: Company D

Bank: Company B

Acct: XXXXXXX9428

Rt: 052000113

Ein: 842375873

Name- K.W."

65. SMITH responded on the same date with a photograph of a Company B receipt in the amount of \$176,407.40, which is the same amount SMITH deposited into the first Company B account on or about July 15, 2019. SMITH then sent YARL the text message "0720" and "Pin."

66. A review of YARL's cellular telephone revealed text messages between YARL

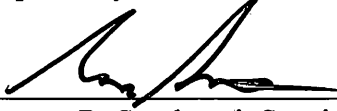
² Sprint lists "Z. Smith" as the subscriber for telephone number (XXX) XXX-8024. The address on the Sprint account is the same address associated with SMITH in law enforcement databases.

and the cellular telephone number (XXX) XXX-0227, which law enforcement confirmed belongs to GHERENSE. On or about July 18, 2019, YARL sent a text message to GHERENSE that said "Boss Groupe LLC" and "Coming." On or about June 20, 2019, YARL sent GHERENSE a text message containing a screenshot of an email from an apartment rental company. The email was directed to K.P., which was a name that YARL used to open the second Company B account under the name Boss Groupe LLC on July 18, 2019.

67. Based on my training and experience, I believe that YARL's communications with SMITH and GHERENSE were in furtherance of a conspiracy to defraud Company B.

68. Based upon the information set forth in this Affidavit, your affiant respectfully submits that probable cause exists to arrest and charge CHEA S. YARL, CAESAR E. ADIGWE, JR, SAMUEL B. SMITH, JR, and THOMAS GHERENSE with conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349.

Respectfully submitted,



Gregory R. Settducati, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on this 13th day of December, 2019: /s/ _____
Theresa Carroll Buchanan
United States Magistrate Judge

The Honorable Theresa Carroll Buchanan
United States Magistrate Judge